Statement of Work

Task Reference No.: T269

Task Name: Information System Security Officer Support for MMAC Backbone, IAP and Voice Systems

Work Originator: AMI-400

Date: 09/29/2010

Task Type: Firm Fixed Price - Level of Effort

Period of Performance: 03/01/2011 – 02/29/2012

Work is to be accomplished for the Federal Aviation Administration (FAA), Mike Monroney Aeronautical Center (MMAC), Office of Information Technology (AMI-1).

1.0 Introduction.

1.1 Organization:

1.1.1 Identification: Department of Transportation (DOT)/Federal Aviation Administration (FAA), Office of Information Technology (AMI-1), Telecommunications Division, AMI-400).

1.1.2 Mission: This administration provides for the regulation and promotion of civil aviation to better foster the development and safety and provide for the safe and efficient use of airspace.

1.2 Project Background and Objectives:

The Office of Information Technology (AMI-1) provides data processing support, including system design, programming, implementation and system support for the Mike Monroney Aeronautical Center, the Federal Aviation Administration, the Department of Transportation, and other governmental agencies and departments.

AMI-400 provides information system security services and resources for the user community when information needs and support services materialize. The services include life cycle management of the data Backbone, Internet Access Point (IAP) and Voice communications systems at the Aeronautical Center.

2.0 Information System Security Services Required

2.1 Scope of Work

Support in the development of policies, procedures and test plans is the role of the Information Systems Security Officer (ISSO). The ISSO also makes periodic assessment of compliance to existing policies and procedures. The ISSO also supports external assessments such as the annual SAS70 and IG audits. The ISSO works with other ISSOs in developing Memorandums of Understanding concerning expected security processes.

2.2 Statement of Work

The contractor will provide the level of support required by AMI-400 for ISSO services over the Backbone, IAP and Voice communications services.

The work will consist of supporting the "Continuous Monitoring Phase" as defined in chapter 5 of the U.S. Department of Transportation Federal Aviation Administration Information Security Certification and Accreditation (C&A) Handbook, dated March 9, 2009 (https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/iss/accreditation/media/C_A_Handbook_030509.doc).

The milestones will overlap and be running concurrently and must be **reviewed and acted on at a minimum of once per calendar year**. The milestones are not in priority order.

Milestone 1. Review existing Security Policy and Procedures for the IAP/Backbone for completeness and satisfaction with reference to NIST guidance.

Milestone 2. Review existing Security Policy and Procedures for the Voice System for completeness and satisfaction with reference to NIST guidance.

Milestone 3. Propose modifications to the ISSO to update policies in coordination with DOT and FAA Policy as well in coordination with NIST guidance.

Milestone 4. Propose modifications to the ISSO to update procedures in support of policies, existing or updated through Milestone 3.

Milestone 5. Propose modifications to the ISSO to update policies in coordination with DOT and FAA Policy as well in coordination with NIST guidance.

Milestone 6. Prepare documentation reflecting implementation of Policies and Procedures. Provide assessment of adherence to Policies and Procedures.

Milestone 7. Work with others to mitigate deficiencies as found through assessment.

2.3 Deliverables:

1. Work will conform to requirements established and referenced in Paragraph 5.0, Applicable Laws and References. National Institute of Standards guidance will be used as primary references as supplemented by DOT and FAA orders. A quarterly report will be provided by the Contractor with milestone dates to meet the standards. All NIST Standards referenced in the Statement of Work can be accessed at http://csrc.nist.gov/publications/PubsSPs.html. Once you access the NIST publications home page, links to all NIST Standards are presented in descending numerical order.

2. Detailed documentation of Information System Security Plans, Policies and Procedures as prescribed in the latest revisions of NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems. Minimally, the Information System Security Plan (ISSP) will be updated once per Calendar year by August 31.

3. Documentation of assessment results and recommendations per NIST SP 800-53A - Guide for Assessing the Security Controls in Federal Information Systems, July 2008. Plans, Actions and Milestone (POA&M) status will be reviewed and reported monthly and updated once per year by August 31.

4. Detailed test plans and results for Cyber Incident response testing per latest revisions of NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment and NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. Disaster Recovery Plan, Training and Testing will be completed annually. The documentation shall be included with the ISSP and updated once per calendar year by August 31.

5. Memorandum of Understandings (MOU/ISA) concerning interconnection of systems, security services levels, per NIST SP 800-47, Security Guide for Interconnection of Security Systems. A quarterly report of outstanding MOU/ISA will be provided. Completed MOU/ISA will be submitted for approval and filed with ISSP by August 31 each calendar year..

6. Continuous reviews will be performed and changes will be performed not less than annually and in accordance with the Department of Transportation Office of Inspector General annual audits. Major reviews will be performed concurrently with independent reviewer as required for Annual Assessment and Re-Certification. Notice of Findings Reports (NFR) status with plans for resolution will be reviewed annually by August 31.

2.4 Qualifications

2.4.1 Information System Security

A working knowledge of several of the following areas is required: understanding of business security practices and procedures; knowledge of current security tools available; knowledge of Windows Network Operating Systems; knowledge of LAN/WAN technology; understanding of Internet Protocols such as TCP, SSH, HTTP and SSL.

2.4.2 Functional Skills

Very good human relations skills associated with information system security involvement of the user community are required. They are expected to communicate the information system security requirements to a community of diverse backgrounds and Information Technology expertise.

2.5 Travel

2.5.1 Travel and Per Diem

Travel may be required for this task. All travel will be coordinated and approved in advance by the Contracting Officer in accordance with the terms and conditions of the contract.

3.0 Facilities, Supplies, and Services

The FAA will give contractor personnel access to its ADP Facilities during normal duty hours during the duration of this task. The contractor's use of these facilities must be directly associated with the task accomplishments.

The FAA will provide desk space, microcomputer (as required) and phone service for the contractor's use associated with task accomplishment.

The task shall be performed on site at the following government installation:

DOT/FAA Mike Monroney Aeronautical Center
6500 S MacArthur Blvd.
Oklahoma City, Oklahoma 73169

3.1 Hours of Work

Normal Duty Hours:

Services are to be performed on-site Monday through Friday (excluding federal holidays and facility closures) between the operating hours of 0600 to 1800.

Shift Duty Hours:

There are three anticipated shift changes per contract year for out of hours testing of some DR processes. When applicable, services are to be performed on-site either Sunday through Thursday or Tuesday through Saturday (applicable schedules to be coordinated between the COTR and Contractor Task Lead) between the operating hours of 0600 to 1800. The contractor will be notified two (2) weeks prior to any shift change.

The task leader must insure adequate resource (contractor) coverage each normal business day or each day affected by a shift change.

3.2 Security Clearance

Contractor personnel assigned to this task will be required to have a level (6) six security clearance.

4.0 Special Instructions

4.1 Inventory, Management, and Control

All information system security support and documentation are to be considered as deliverables to the represented MMAC organization

4.2 Documentation

The contractor will provide and maintain documentation which can be utilized to outline trends, problems, maintenance requirements, software or module changes for current or future support of MMAC microcomputers, LAN's and WAN's, and enhancements. The contractor will also provide daily updating for reference and information system security evaluation material used in support of MMAC microcomputers, LAN's, WAN's, and local data support projects.

4.3 Quality Control and Information System Security Issues

The contractor will provide support for all reported problems, software changes/modifications, and hardware changes/modifications. Quality control procedures will be approved by AMI-400.

4.4 Access to Project Material

Contractor support assigned to this task will have access to all documentation, software, and information system security material required in the performance of this task.

5.0 Applicable Laws and References

- Federal Information Security Management Act (FISMA) of 2002 (http://csrc.nist.gov/groups/SMA/fisma/index.html)
- Computer Fraud and Abuse Act of 1986, as amended (http://www.usdoj.gov/criminal/cybercrime/1030_new.html).
- Privacy Act of 1974 (http://www.defenselink.mil/privacy/documents/PrivacyAct1974_Am0702.pdf)
- OMB Circular No. A-130, Appendix III (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
- Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 (http://csrc.nist.gov/publications/PubsFIPS.html)
- NIST Special Publication (SP) 800-18 - Guide for Developing Security Plans for Federal Information Systems, February 2006 (http://csrc.nist.gov/publications/PubsFIPS.html)
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems, January 2002
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems, June 2002 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-53 Rev 2 - Recommended Security Controls for Federal Information Systems, December 2007 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-53A - Guide for Assessing the Security Controls in Federal Information Systems, July 2008 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-60 Rev1 Volume I - Guide for Mapping Types of Information and Information Systems to Security Categories, June August 2008 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-60 Rev1 Volume II – Appendixes to Volume I (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-63 v1.0.2 - Electronic Authentication Guideline, April 2006 (http://csrc.nist.gov/publications/PubsSPs.html)

- NIST SP 800-64 - Security Consideration in the Information System Development Life Cycle, June 2004 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006 (http://csrc.nist.gov/publications/PubsSPs.html)
- NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment, September 2008 (http://csrc.nist.gov/publications/PubsSPs.html)

FAA orders below can be accessed by going to https://employees.faa.gov/tools_resources/orders_notices/ and searching for the specific number identified below.

- FAA Order 1280.1B, Protecting Personally Identifiable Information (PII), December 17, 2008
- FAA Order 1350.15C Records Organization, Transfer, and Destruction Standards, August 29, 2001
- FAA Order 1370.79A FAA Internet Use Policy, October 12, 1999
- FAA Order 1370.82A Information Systems Security Program, September 2006
- FAA Order 1370.84, Internet Services March 4, 2002
- FAA Order 1370.90, Internet Access Point Configuration Management August 1, 2003
- FAA Order 1370.91, Information Systems Security Patch Management, May 19, 2004
- FAA Order 1370.92, Password and PIN Management, June 28, 2004
- FAA Order 1370.94A, Wireless Technologies Policy, September 10, 2008
- FAA Order 1370.95, Wide Area Network Connectivity Security, September 12, 2006
- FAA Order 1370.100, Media Sanitization and Destruction Policy, October 1, 2007
- FAA Order 1370.102, System Use Notification and Disclaimer Statement Policy, July 21, 2008
- FAA Order 1370.103, Encryption Policy, November 12, 2008
- FAA Order 1370.104, Digital Signature Policy, October 31, 2008
- FAA Order 1600.1E, Personnel Security Program, July 25, 2005
- FAA Order 1600.2E, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information, March 13, 2006

- FAA Order 1600.6E, Facility Security Policy, March 11, 2004
- FAA Order 1600.66,Telecommunications and Information System Security Policy, July 27, 1994
- FAA Order 1600.68, FAA Information Systems Security Program, March 5, 1999
- FAA Order 1600.69B, FAA Facility Security Management Program, October 1, 2003
- FAA Order 1600.6C, Physical Security Management Order, April 16, 1993
- FAA Order 1600.6E, Facility Security Policy, March 3, 2004
- FAA Order 1600.72A, Contractor and Industrial Security Program, December 28, 2005
- FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI), February 1, 2005
- FAA Order 1800.66, Configuration Management Policy, September 19, 2007
- FAA Order 1900.1G, FAA Emergency Operations Plan, September 11, 2006